WHAT IS CLAIMED IS:

1. A cryptographic key management method comprising steps of:

generating and storing a management cryptographic key;

generating a transaction cryptographic key;

encrypting the transaction cryptographic key with the management cryptographic key; and

storing the encrypted transaction cryptographic key in a key management server.

2. A cryptographic key management method according to claim 1, wherein if a plurality of transaction cryptographic keys are generated, each of the transaction cryptographic keys is encrypted with the management cryptographic key.

3. A cryptographic key management method according to claim 1, further comprising steps of:

acquiring the encrypted transaction cryptographic key from the key management server;

decrypting the encrypted transaction cryptographic key with the management cryptographic key; and

acquiring the transaction cryptographic key.

4. A cryptographic key management method according to claim 1, wherein the transaction cryptographic key is a pair of a public key and a secret key of a public key cryptographic scheme.

5. A cryptographic key management method

according to claim 4, wherein:

the secret key of the transaction cryptographic key is encrypted with the management cryptographic key and the encrypted secret key and the plaintext public key are stored in the key server; and

the key server checks whether a received public key is coincident with the stored public key, and notifies the check result to a public key sending site.

6. A cryptographic key management method according to claim 3, wherein:

the management cryptographic key is a pair of a public key and a secret key of a public key cryptographic scheme, and the public key of the management cryptographic key is stored in the key server; and

the key server authenticates a requesting site requesting for acquisition of the transaction cryptographic key, by using the stored public key.

7. A network system comprising:

an application server for providing services;

a client for using the services; and

a key server,

wherein:

said client acquires and stores a management cryptographic key, acquires a transaction cryptographic key to be used for a transaction with said application server, encrypts the transaction cryptographic key with

the management cryptographic key, sends the encrypted transaction cryptographic key to said key server, requests the key server to send back the encrypted transaction cryptographic key for the transaction, and decrypts the encrypted transaction cryptographic key with the management cryptographic key to acquire the transaction cryptographic key; and

said key server stores the sent, encrypted transaction cryptographic key and sends the encrypted transaction cryptographic key to said client in response to a request from the client.

8. A network system according to claim 7, wherein when said client acquires a plurality of transaction cryptographic keys different for said respective application servers, said client encrypts each of the transaction cryptographic keys with the management cryptographic key.

9. A network system according to claim 7, wherein:

said client sends a valid term of the encrypted transaction cryptographic key together with the encrypted transaction cryptographic key to the key server; and

said key server notifies an expiration of the valid term of the transaction cryptographic key.

10. A network system according to claim 7, wherein:

said client sends the maximum number of use

times of the transaction cryptographic key together with the encrypted transaction cryptographic key to said key server; and

said key server counts the number of acquisition requests for the encrypted transaction cryptographic key and notifies uses over the maximum number to said client.

11. A network system according to claim 7, wherein:

the management cryptographic key is a pair of a public key and a secret key of a public key cryptographic scheme;

said client stores the public key of the management cryptographic key in said key server; and

said key server authenticates a requesting site requesting acquisition of the management cryptographic key by using the stored public key, and if authentication succeeds, sends the transaction cryptographic key to said requesting site.

12. A network system according to claim 7, wherein:

the transaction cryptographic key is a pair of a public key and a secret key of a public key cryptographic scheme;

said client encrypts the secret key of the transaction cryptographic key with the management cryptographic key and stores the encrypted secret key and the plaintext public key in said server; and

said server checks whether the public key sent from said application server is coincident with the stored public key of said client and notifies the check result to said application server.